

# Security

ADVISOR

MIDDLE EAST

ISSUE 2 | FEBRUARY 2016

[www.securityadvisorme.com](http://www.securityadvisorme.com)



## THE ENEMY WITHIN

HOW TO TACKLE INSIDER THREATS

**cnme**  
computer news middle east  
SUPPLEMENT

**+** Flipping the  
economics of  
attacks

Identifying  
the security  
pitfalls in SDN

How to build  
physical security  
into a data centre



# Hewlett Packard Enterprise



Brought to you by HPE & Intel®.  
Intel Inside®. Powerful  
Solution Outside.

**Build more than  
infrastructure.**  
**Build revenue.**

HPE Converged Systems transforms  
IT into an agile foundation for  
better business results:

Business services up and running in  
weeks vs. months\*

- Nearly 2X staff productivity\*
- 315% ROI\*
- 40% lower TCO\*

Faster, simpler, and more efficient,  
HPE Converged Systems help businesses  
spend more time building new revenue  
streams—and creating a real competitive  
advantage.

For more info: [www.hpe.com](http://www.hpe.com)



**FOUNDER, CPI MEDIA GROUP**  
Dominic De Sousa (1959-2015)

**Group CEO**  
Nadeem Hood

**Publishing Director**  
Rajashree Rammohan  
raj.ram@cpimediagroup.com  
+971 4 375 5685

## EDITORIAL

**Group Editor**  
Jeevan Thankappan  
jeevan.thankappan@cpimediagroup.com  
+971 4 375 5678

**Editor**  
Annie Bricker  
annie.bricker@cpimediagroup.com  
+971 4 375 1643

**Deputy Editor**  
James Dartnell  
james.dartnell@cpimediagroup.com  
+971 4 375 5684

**Online Editor**  
Adelle Geronimo  
adelle.geronimo@cpimediagroup.com  
+971 4 375 5683

## ADVERTISING

**Commercial Director**  
Chris Stevenson  
chris.stevenson@cpimediagroup.com  
+971 4 375 5674

**Group Sales Director**  
Kausar Syed  
kausar.syed@cpimediagroup.com  
+971 4 375 1647

**Sales Manager**  
Merle Carrasco  
merle.carrasco@cpimediagroup.com  
+971 4 375 5676

## CIRCULATION

**Circulation Manager**  
Rajeesh M  
rajeesh.nair@cpimediagroup.com  
+971 4 375 5682

## PRODUCTION AND DESIGN

**Production Manager**  
James P Tharian  
james.tharian@cpimediagroup.com  
+971 4 375 5673

**Designers**  
Analou Balbero  
analou.balbero@cpimediagroup.com  
+971 4 375 5680

Neha Kalvani  
neha.kalvani@cpimediagroup.com  
+971 4 375 1644

## DIGITAL SERVICES

**Web Developer**  
Jefferson de Joya  
Abbas Madh  
  
**Photographer**  
Charls Thomas  
Maksym Poriechkin  
  
webmaster@cpimediagroup.com  
+971 4 440 9100

Published by



Registered at IMPZ  
PO Box 13700  
Dubai, UAE

Tel: +971 4 440 9100  
Fax: +971 4 447 2409

Printed by  
Al Ghurair Printing & Publishing

Regional partner of



© Copyright 2016 CPI  
All rights reserved

While the publishers have made every effort  
to ensure the accuracy of all information  
in this magazine, they will not be held  
responsible for any errors therein.

# CONTENTS



## 04 INSIDE JOB

The IT threat landscape has been evolving at an unprecedented pace. We take a look at the menacing impacts of insider threats.

## 10 FLIPPING THE ECONOMICS OF ATTACKS

A research study on the pecuniary motivations of cyber attacks and how they can be thwarted.

## 20 ASSESSING SAAS APPLICATIONS

Smartsheet's Ken Asher shares the seven goals a SaaS security review should address.

## 14 SECURITY PITFALLS OF SDN

Industry experts delve into the vulnerabilities that can be caused by software-defined networks.

## 22 FIGHTING CYBERWARFARE

A10 Networks gives insights on how government agencies can keep state-sponsored attacks at bay.

## 18 PHYSICAL SECURITY INTO A DATA CENTRE

Top tips CSOs should consider in ensuring that the physical space of the data centre is built with security in mind.

## 24 MODERN DEFENCE

RSA Security's Zulfikar Ramzan on adapting to the changes in the threat landscape and the value-add security can bring to businesses.





# INSIDE JOB

These days, the threat landscape for most companies is massive. But while there is a litany of outside threats that their security teams need to worry about, there is often an even greater danger much closer to home.

## R

egardless of your industry, the size of your organisation, or

the type of business you have, insider threat is a menacing reality. In most organisations, this threat has been undervalued, underestimated and underfunded. It's the elephant in the room that no one wants to talk about because it means acknowledging that one of your own employees might take you for a ride.

Security pros are constantly being warned about insider threats. We were that told our companies need next-generation software, integrated threat intelligence, and the ability to correlate massive amounts of event logs and context to arm ourselves against these threats.

We were told that these tools are necessary to block attacks and to recover from attacks, should they be successful. Unfortunately, when companies eventually figure out that they've been compromised, they also discover their

systems had been compromised for an extended period of time.

"Insider threats can include a combination of malicious insiders, compromised insiders, and careless insiders," says Wade Williamson, Director, Product Marketing, Vectra Networks. "You will need clear visibility for identifying all of these threats, but they will differ in behaviour and how security will be able to detect them."

Just how big is the insider threat problem?

According to the Cisco Connected World Technology Report, seven of out of 10 employees admitted to knowingly breaking IT policies on a regular basis, and three out of five believe they are not responsible for protecting corporate information and devices.

"According to some estimates, up to 90 percent of organisations are not fully aware of devices accessing their network; and it is not unusual to learn that there are five to 10 times



**"Emerging technologies, tools and connectivity, mobile and remote working, all mean that insiders now have new ways of coordinating with others."**

*- Greg Day, VP & CSO, Palo Alto Networks EMEA*

more cloud applications in use than IT departments realise. In addition, there is an increasing number of devices connecting to the network, resulting for challenges to grow exponentially," says Anthony Perridge, Security Sales Director, Cisco.

Nicolai Solling, Director, Technology Services, Help AG, cites a recent study from Crowd Research that says over the last year, 62 percent of security professionals found insider threats have become more frequent. Despite this, fewer than 50 percent of organisations have appropriate controls to mitigate this threat.

"This is of course closely linked to the fact that when a company starts up an employment relationship with an individual it is based on the assumption and trust that the person is the correct one to do a job," he adds. "Insider threats are generally difficult to detect as they are different in autonomy than other threats and can therefore circumvent our classical defense systems. Typically, insider threats are focused on data leakage



**"Insider threats are focused on data leakage over prolonged periods of time, as an example it could be intellectual property and trade secrets. As the employee also takes data in and out of the organisation in the form of mobile devices and laptops there it is also difficult to physically monitor the behavior of the individual."**

*- Nicolai Solling, Director of Technology Services, Help AG*

over prolonged periods of time, as an example it could be intellectual property and trade secrets. As the employee also takes data in and out of the organisation in the form of mobile devices and laptops there it is also difficult to physically monitor the behaviour of the individual."

When it comes to security, insider threats are an unfortunate fact of life, and there are many factors increasing organisations' exposure to threats posed by insiders. "Enterprises are finding it more and more difficult to protect their networks for a number of reasons. First, the increasing use of BYOD (bring your own device), where employees use their own smartphones and tablets in the office, means that the boundary between trusted and untrusted devices is becoming ever more difficult to define," says Simon Bryden, Consulting Systems Engineer, Fortinet.

Raj Samani, VP and CTO, Intel Security EMEA, explains that one of the main factors increasing exposure is the openness by which employees are willing to share information about themselves or the company online. This allows anyone to conduct research on their target within minutes.

Greg Day, VP and CSO, Palo Alto Networks EMEA, adds that emerging technologies, tools and connectivity, mobile and remote working, all mean that insiders now have new ways of coordinating with others. For example,

the number of SaaS-based applications observed on enterprise networks has grown 46 percent from 2012 to 2015, and now includes more than 316 applications. "The scope of internet based applications and services will only continue to grow, and whilst businesses have been used to managing their own environment, cloud services require new ways of security thinking. It's all too easy to feel you have lost control which simply isn't the case."

Because most insider activity is never identified, many organisations do not see it as high priority. Yet, an insider carrying out a malicious plan can leave with clean hands and bags full of an organisation's asset. Even when caught, CERT reports that 82 percent of the time remediation is handled internally with no legal action. This is likely to avoid unwanted public scrutiny or other potential fall out for the organisation due to the incident.

"Alienating employees is perhaps the biggest threat. The wrong implementation of a mobile authentication solution could result in severely compromised convenience for a company's user base, resulting in an extremely poor user experience. While security is tightened, perhaps through multiple passcodes and other authenticators, employees are likely to resent the time consuming procedures they need to go through in order to access corporate data. As a result, they'll likely resort to sharing compromising



**"One of the main factors increasing exposure is the**

**openness by which employees are willing to share information about themselves or the company online. This allows anyone to conduct research on their target within minutes"**

*- Raj Samani, VP and CTO, Intel Security EMEA*

data through alternative channels outside of an authenticated pathway,” explains Marc Hanne, Director of Sales, Identity Assurance, HID Global.

There may be no single solution to the complex challenge of protecting against insider threats within the enterprise, but IT leaders can help their cause with prudent policies that limits on who can access what kinds of data, and working to boost awareness of security issues throughout the organisation.

For a new or rehabbed insider threat programme to be successful, the CIO, CISO or CSO first has to gain boardroom buy-in and illuminate the value such a programme would have to a company in detecting and preventing harm to people, property and company reputation. A thorough assessment of the known or existing vulnerabilities and threats, weighed against the overall company risk appetite, is essential.

“Many organisations develop a user awareness programme, but the effectiveness of such programmes varies,” says Samani. “An awareness programme that is combined with measures to evaluate its effectiveness is one of the best tools for fighting social engineering attacks. Although continuous measurement and refinement in education programmes represent an effective counter against social engineering, they are rarely used. In fact, many organisations have not implemented any sort of



**“Technologies such as device management, encryption or data-loss prevention can help reduce the risk of an insider threat - but we must keep in mind that it is impossible to completely eliminate this risk.”**

*- Stefan Tanase, Senior Security Researcher at Kaspersky Lab*

security or policy awareness training for their employees.”

Stefan Tanase, Senior Security Researcher, Kaspersky Lab, offers another perspective, “If we assume that an insider is planning to leak internal corporate documents, during the days or weeks in which the actual information gathering process occurs, his actions could be detected by observing anomalies in his behavioural patterns - whether it is network activity, such as fetching local copies of a large number of internal documents via company intranet, or even real-life clues, such as using the copying machine more often than usual.”

Technologies such as device management, encryption or data-loss prevention can help reduce the risk of an insider threat - but we must keep in mind that it is impossible to completely eliminate this risk. A highly motivated insider with the right tools and access could always pose a threat, he adds.

Some companies shy away from implementing an insider threat programme because they worry about the cost of technology to back it up would be prohibitive or that it would be too cumbersome for employees.

But experts say insider threat programmes can be implemented in most part by removing privileged access where it is not needed or too risky, and by using the tools already embedded in the network.

Day from Palo Alto Networks says, “For any insider threat programme to work, it must rely on humans communicating policies clearly across business boundaries, from the executive leadership team down to employees. All business functions starting from the internal business units to the external trusted business partners should be informed about acceptable use. Everyone must be onboard from the managers observing employee behaviour and reporting anomalies to both human resources and from the IT department gathering evidence for leadership to make a decision.”

The best approach to combat the menace of insider threats is to make sure that your company’s security policies clear and accessible to all employees. They should also be actively enforced. Employees have to be constantly reminded of the policies and why the restrictions are in place, despite the inconvenience it may cause. In general, companies need to take a 360-degree view of security that encompasses internal and external threats. 🔒



**“Enterprises are finding it more and more difficult to protect their networks for a number of reasons. First, the increasing use of BYOD (bring your own device), where employees use their own smartphones and tablets in the office, means that the boundary between trusted and untrusted devices is becoming ever more difficult to define.”**

*- Simon Bryden, Consulting Systems Engineer, Fortinet*





ENJOY SAFER TECHNOLOGY™

# DO MORE

# WITH YOUR I.T. SECURED BY ESET

Whether you're managing your business, or overseeing your company's IT, ESET's security products are fast, easy to use, and deliver market-leading detection. We deliver the protection that allows you to DO MORE. Find out more at [ESET.COM/ME/BUSINESS](https://www.eset.com/me/business)

# LARGE DATA BREACHES REPORTED IN 2015


High-profile security breaches continue, keeping cybersecurity top of mind. A huge number of companies, academic institutions and government agencies around the world have been breached proving that information is not always safe. Here are some of the biggest data breaches reported in the past year.



**50,000  
COMPROMISED  
RECORDS**



**1,000,000  
COMPROMISED  
RECORDS**



**50,000**



Uber found that a database containing approximately 50,000 drivers' names and licence numbers was accessed by a third party and was forced to change access protocols.



**50,000**




The computer system of FireKeepers Casino Hotel were breached and 85,000 credit and debit cards between September 2014 and April 2015 may have been compromised.



**104,000**



An unnamed cybermafia used the IRS website to obtain on personal information on 104,000 taxpayers and claimed 15,000 tax refunds in other people's name.



**150,000**




Advantage Dental was breached and cybercriminals were able to steal the names, dates of birth, Social Security numbers and home addresses of 150,000 patients.



**160,000**




Cybercriminals gained access to nearly 160,000 current and former students' personal information from Metropolitan State University, including addresses, phone numbers and GPAs.



**400,000**



mSpy, a software that let users spy on mobile devices, was breached and emails, text messages, payment and location data on nearly 400,000 users were exposed.



**900,000**



HanesBrands was breached and cybercriminals accessed addresses and phone numbers of 900,000 customers. Email addresses and full credit card numbers were not compromised.




**20,000,000**


The username and email messages of 20 million visitors were stolen from Topface, dating website in Russia. Topface paid a ransom to the attacker not to expose the information.


**21,500,000**


The government had Social Security numbers and other sensitive information on 21.5 million people stolen from the computer networks of the Office of the Personnel Management.


**37,000,000**


The data of 37 million users of the infidelity site of Ashley Madison was posted online by the group that claimed to have completely compromised the company's database of users.


**40,000,000**


The writing community Wattpad was breached and the log-in information of 40 million users were compromised. Users were prompted to update their passwords.


**80,000,000**


Anthem, the country's second largest health insurer, was attacked and the names, dates of birth, addresses and Social security numbers of 80 million customers were compromised.

Data breaches make headlines nearly everyday.  
Awareness of security is at an all-time high, and enterprises are continuously looking for new solutions.

# FLIPPING THE ECONOMICS OF ATTACKS

How much does it cost technically proficient adversaries to conduct successful attacks, and how much do they earn? The research study from Ponemon Institute, commissioned by Palo Alto Networks, looks at the relationships between the time spend and compensation of today's adversaries and how organisations can thwart attacks.

A

s revealed in this research, while some attackers may be motivated by

non-pecuniary reasons, such as those that are geopolitical or reputational, an average of 69 percent of respondents say they are in it for the money.

In this study, we surveyed 304 threat experts in the United States, United Kingdom and Germany. We built this panel of experts based on their participation in Ponemon Institute activities and IT security conferences. They were assured their identity would remain anonymous. Twenty-one percent of respondents say they are very involved, and 79 percent of respondents are involved in the threat community. They are all familiar with present-day hacking methods.

#### **Attackers are opportunistic.**

Adversaries go after the easiest targets first. They won't waste time on an attack that will not quickly result in a treasure trove of high-value information, according to 72 percent of respondents. Further, attackers will quit when the targeted company has a strong defense, according to 69 percent of respondents.

#### **Cost and time to plan and execute attacks are decreasing.**

According to 53 percent of respondents,

the total cost of a successful attack has decreased, driving even more attacks across the industry. Similarly, 53 percent of respondents say the time to plan and execute an attack has decreased. Of these 53 percent of respondents who say it takes less time, 67 percent agree the number of known exploits and vulnerabilities has increased, 52 percent agree attacker skills have improved and 46 percent agree hacking tools have improved.

#### **Increased usage of low-cost and effective toolkits drives attacks.**

Technically proficient attackers are spending an average of \$1,367 for specialised toolkits to execute attack. In the past two years, 63 percent of respondents say their use of hacker tools has increased and 64 percent of respondents say these tools are highly effective.

**Time to deter the majority of attacks is less than two days.** The longer an organisation can keep the attacker from executing a successful attack the stronger its ability to safeguard its sensitive and confidential information. The inflection point for deterring the majority of attacks is less than two days (40 hours) resulting in more than 60 percent of all attackers moving on to another target.

**Adversaries make less than IT security professionals.** On average, attackers earn \$28,744 per year in annual compensation, which is about one-quarter of a cybersecurity professional's average yearly wage.

#### **Organisations with strong defenses take adversaries more than double the time to plan and execute attacks.**

The average number of hours a technically proficient attacker takes to plan and execute an attack against an organisation with a 'typical' IT security infrastructure is less than three days (70 hours). However, when the company has an 'excellent' IT infrastructure the time doubles to an average of slightly more than six days (147 hours).

**Threat intelligence sharing is considered the most effective in preventing attacks.** According to respondents, an average of 39 percent of all hacks can be thwarted because the targeted organisation engaged in the sharing of threat intelligence with its peers.

**Investments in security effectiveness can reduce successful attacks significantly.** As an organisation strengthens its security effectiveness, the ability to deter attacks increases, as shown in this report. The following are recommendations to harden organisations against malicious actors:

- Create a holistic approach to cyber security, which includes focusing on the three important components of a security programme: people, process and technology.
- Implement training and awareness programmes that educate employees on how to identify and protect their organisation from such attacks as phishing.
- Build a strong security operations team with clear policies in place to respond effectively to security incidents.
- Leverage shared threat intelligence in order to identify and prevent attacks seen by your peers.

**“The longer an organisation can keep the attacker from executing a successful attack the stronger its ability to safeguard its sensitive and confidential information.”**



- Invest in next-generation technology such as threat intelligence sharing and integrated security platforms that can prevent attacks and other advanced security technologies.

#### The economic motivation of attackers

- What motivates an attacker? 69 percent of respondents in this study are motivated by money. While many attackers may be hoping for a big 'payout,' reality can be quite different. The findings reveal that attackers on average receive \$28,744 for an average of 705 hours spent on attacks annually.
- Of course, some attackers do 'earn' more than the average. However, this compensation is 38.8 percent less than the average hourly rate of IT security practitioners employed in the private and public sector.

#### Inflection point: When malicious actors call it quits

Time to deter the majority of attacks is less than two days. The survey asked respondents how much time it takes to plan and execute web-based and malicious code attacks and if the time has increased, decreased or stayed the same. The study also examines how many of these attacks are successful and when does an attacker call it quits.

The longer an organisation can keep the attacker from executing a successful attack, the stronger its ability to safeguard its sensitive and confidential information. While no organisation has unlimited resources to spend hardening itself against malicious actors, understanding the amount of time until attackers' efforts are no longer potentially profitable will help the leadership prioritise investments in the appropriate technologies.

Time is the enemy of an attacker. The more time that passes before a successful attack can execute, the more likely an organisation can stop it. For example, a delay of five hours

**“Time is the enemy of an attacker. The more time that passes before a successful attack can execute, the more likely an organisation can stop it.”**

in conducting a successful attack deters 13 percent of attacks, a delay of 10 hours can reduce 24 percent of attacks, and 20 hours deters 36 percent of attacks. On average, a technically proficient hacker will quit an attack and move to another target after spending less than nine days without success.

#### Hardening the organisation against attackers

Threat intelligence sharing is considered most effective in preventing attacks. To make it more difficult to execute a successful attack, the solution is to exchange threat intelligence with peers and to invest in the appropriate technologies to strengthen an organisation's security posture. An average of 39 percent of all hacks can be thwarted because the targeted organisation engaged in the sharing of threat intelligence with its peers. Additionally, out of all technologies available, threat intelligence sharing was cited by 55 percent of respondents as the most likely to prevent or curtail successful attacks.

It is clear the attack landscape has changed. Each day we see more successful data breaches against organisations around the globe. This study has exposed as important element of this criminal underground, which can often be missed when headlines about the next Big Data

breach dominate the front page: the economic motivation of cybercriminals and how we can use this information to turn the tables on them. The findings clearly show the profit-based motivation of attackers, which means the same economic forces are at work for them as for major businesses. Adversaries are in it for the quick and easy payday, with the majority of them making far less than comparable IT security professionals.

Ponemon Institute expects the cost of attacks to continue to decrease, as attackers become more skilled and automated toolkits are improved and in widespread use, as well as other factors examined in this survey. There is another side to the cost equation though, which the security community can use to keep it safe. We can change the economics of attacks, by putting up a better defense, which takes attackers much longer to overcome.

This survey has shown how attackers will divert their attention to other targets after an increase in the time it takes to breach an organisation of less than two days. Like many businesses, adversaries are constantly weighing the potential profit versus cost, which includes the time it takes them to be successful. As a security community, we must take into account the motivation and economic environment surround attacks, not just technical solutions to the problem. 🔑



# Simplify IT fast. Get back to business faster.

**How to simplify IT with HP hyper-converged systems.** Now your business can quickly realize the simplicity of IT convergence.

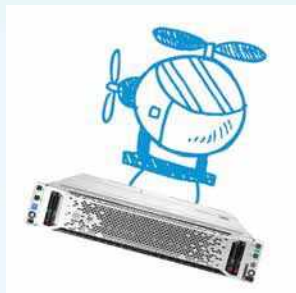
- Step one: Open the box
- Step two: Power-on new IT infrastructure—servers, storage, networking—instantly
- Step three: Shift focus from maintenance to revenue-boosting innovation

Hyper-convergence is that simplified. Make your business out-of-the-box fast. So you can spend more time creating opportunity, not just reacting to it.

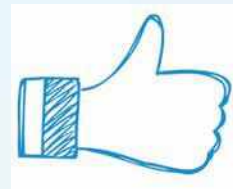
For more info: [www.alpha.ae](http://www.alpha.ae)



1. Unbox



2. Deploy



3. Provision in 15 minutes



Brought to you by HPE & Intel®.  
Intel Inside®. Powerful Solution Outside.

Based on internal testing, January 2015 of an HP ConvergedSystem 200-HC StoreVirtual with HP OneView for vCenter version 7.40, HP OneView InstantOn version 1.00, and VMware vCenter Server version 5.5.  
© 2015 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. Intel and the Intel logo are trademarks of Intel Corporation in the U.S. and/or other countries.



# IDENTIFYING THE SECURITY PITFALLS IN SDN

While a software-defined network can improve application performance and help ease administrative tasks, it can also create new vulnerabilities. Experts offer advice for security teams.





**S**oftware-defined networks can be a boon to savvy organisations,

offering opportunities to cut administrative costs while increasing network agility. But SDN technology can also create security risks, and how you manage those risks can mean the difference between a successful implementation and a disastrous one.

With the SDN architectural model, control of a network is decoupled from the physical infrastructure, which enables administrators to manage network services across different types of equipment from multiple vendors. Organisations can decouple the system that makes decisions about where traffic goes (control plane) from the systems that forward traffic to selected destinations (data plane).

SDN can deliver automated provisioning, network virtualisation and network programmability to data centre and enterprise networks. The increased network flexibility can help organisations as they move further into areas such as cloud computing, mobile technology and the Internet of Things.

"SDNs are the new architecture for the new age of IT and [off-premises] processing," says Daniel Mikulsky, an IT disaster recovery instructor at the Disaster Recovery Institute International, which provides professional certifications and education programmes. "With the rise of cloud services, Big Data and the consumerisation of IT through mobile computing and the Internet of Things, network flexibility and adaptability need to coincide with other innovations in technology."

Demand for the technology is expected to rise: IDC estimates the worldwide SDN market will hit \$8 billion by 2018. That forecast includes physical network infrastructure that's already in use, controller and network-virtualisation software, SDN network and security services and related applications, and SDN-related professional services.

And as demand for SDN grows, so too do security fears.

"One of the biggest security issues is that this is still a relatively immature technology, so we don't know for sure what types of exposures are possible," says Frank Cervone, Director of IT, School of Public Health, University of Illinois, Chicago.

But while there's still much to learn about SDN, security experts who have begun to explore the technology's hidden dangers say there are ways to safeguard your systems.

### **A technology in layers**

While the technology is relatively new, specific vulnerabilities already have been identified within the SDN architecture, particularly the data plane and controller layers.

In the data plane layer, many of the protocols are still new, "so we don't know how robust they really are," Cervone says. "Some of the protocols do not require authentication or encryption, so it's possible that an incorrectly configured component on the network could become an attack vector, inadvertently allowing traffic to be diverted or inspected."

The data plane layer, as with SDNs in general, can also be vulnerable to outages in a natural or man-made disaster. "Given that most major disasters are regional, which will cause physical disruption of network infrastructure, SDNs will need to be configured to meet normal capacity," Mikulsky says.

However, because disaster recovery is becoming increasingly network-dependent, "we can't be sure that the reconfigured network can cope with the additional demands on capacity," he says.

Companies need to ask their network providers if they have contingency plans to add capacity in the event of a disaster. Virtualisation is one way to redirect resources, Mikulsky says, but physical capacity needs to be available and accessible.

Also in the data plane, some older data centre access technologies are deployed, including tunnels, Virtual Extensible LANs and a variety of bridging protocols, says Chris Krueger, Director, Cloud and Virtualisation, Coalfire, a provider of risk management and compliance services.

"Hackers capturing these streams can gain insight into the network implementation, as a result of their payloads being unencrypted and often poorly segmented or secured," Krueger says. "By monitoring and then forging the Data Centre Interconnect link traffic, a variety of disruptive and intrusive events may be perpetrated."

#### Targeting the control plane

Security risks are magnified within the control plane, because "it becomes a single point of failure in an SDN environment and relies heavily on automation," says Stan Mesceda, High-speed Encryption Product Manager, Gemalto, a security technology vendor.

"If the controller is compromised, there are risks of denial of service, misdirected traffic and [exposure of] data at rest or in transit," Mesceda says. "Also, human errors within an SDN controller or orchestration engine can have a ripple effect throughout the network."

SDN controllers will likely prove to be high-value targets, although again, it's too soon to know what kinds of attacks companies could suffer, says

Brad Hibbert, CTO, BeyondTrust.

"Most vulnerabilities that are leveraged in the wild have patches, but [the patches] have not been deployed due to resource limitations, lack of process and so on," Hibbert says.

"When you are talking about network equipment and hypervisors that, if compromised, can have a devastating impact on the risk posture of an organisation, these are items that need to be of highest priority and included in your ongoing vulnerability management and patching programme."

Another significant vulnerability continues to be excessive access and lack of administrative oversight on networking equipment and hypervisors, both on-premises and in the cloud.

"As insiders and outsiders through a compromised account, have direct access to manage such network and data centre components, they can not only impact availability but also open channels to allow malware and information to slip through and be exfiltrated out of the organisation," Hibbert says.

With a typical network, the rule of least privilege is important, adds Chase Cunningham, threat intelligence lead at cloud hosting company Armor. "But with an SDN system, if any one user is granted rights to something they shouldn't have access to, the whole network and literally every asset, item, configuration and database are in danger."

All it takes is a small incorrect

configuration and a malicious user. Or an infected machine could access and control or modify items well outside the scope of their intended uses, Cunningham says.

"Malware that can detect if it is on a virtual host and try and 'hop' to the actual control server or entity is also a concern," he says. "That could be an apocalypse scenario, as the malware could theoretically have command and control of everything that is running on the SDN and the entire virtual environment."

One of SDN's benefits is its ability to adaptively respond to a distributed denial-of-service attack, Cervone says. "The software can simply adjust the structure of the network to circumvent the attack rather than just trying to block the attack, which is a significant improvement over past strategies," he says.

But the SDN software stack itself could also be attacked, Cervone says. "If someone were to develop a mechanism that could flood the stack so that it went into overdrive trying to reconfigure the network, thinking that a different type of attack was going on, that could certainly make the network grind to a halt."

#### Locking down SDN environments

Here's a look at some specific recommendations security experts have for companies planning to deploy SDN technologies.

Be proactive about SDN security. As SDN becomes more common, the attack vectors will likely increase. Organisations need to be prepared for the vulnerabilities and take steps to mitigate them.

You should have a predefined security plan ready when you begin designing a network, Krueger says. Include architectural mandates, and security appliance/device implementation guidelines that have been vetted by your company's chief information security officer and are in keeping with policies and directives.

"Use of SDNs will become

**"Hackers capturing these streams can gain insight into the network implementation, as a result of their payloads being unencrypted and often poorly segmented or secured."**

widespread in the near future, and by virtue of cloud providers becoming the actual infrastructure for more business-critical workloads, this topic will have greater focus, interest and exposure in the years to come," Krueger says. "Make security a design-in before you build it. Break the cycle of adding security as an afterthought, if that's been the model thus far."

Standard security practices can be implemented to keep SDNs secure, Mikulsky adds. "These entail rigid policy implementation and control, monitoring, scheduled patching and maintenance, as well as the implementation of moving-target defense algorithms," he says.

However, with SDN security, you should adopt exercise and testing scenarios that assume that an attack has been successful. Procedures should include detecting the anomaly, isolating the problem from the rest of the healthy network, and then implementing automated self-healing within the network.

Practice vigilance with network access and user authentication. "The most overt issue with SDN is really careful management of the configuration and ensuring that only those users who need access to certain items or areas of the network are provided that access," Cunningham says.

"Lock down permissions, and double-check regularly that they are configured correctly," he says.

As for authentication, "make sure users are who they say they are but also authenticate applications" and network-function virtualisation, Mesceda says. "As new circuits or applications are spun up, make sure that the architecture and applications riding on it are secure and performing as desired."

Maintain the visibility of all of the layers. "The best practices applied to SDN should follow those related to cloud computing and network infrastructure security," says Chris Richter, Senior Vice President, Managed Security Services,

**"Make security a design-in before you build it. Break the cycle of adding security as an afterthought, if that's been the model thus far."**

Level 3 Communications, a global communications network operator.

"Level 3's approach to tackling these issues is a multi-tiered, network-based model," Richter says.

Having visibility into the individual layers, how they interact with each other and what systems have access to these layers "is key to detect abnormal activities," he explains. "You cannot defend yourself against something you can't see. Once you can see what is happening, you can determine the appropriate counter-measure."

In addition, it's imperative to have a clear definition of who administers the policy for each layer. "A strong orchestration engine can be designed to balance the business and security needs, but security policies should outline which security functions will be automated," Mesceda says.

Make note of changes as you move to SDN. Cunningham advises establishing a firm and detailed system baseline as the migration to an SDN environment takes place. "Without good knowledge of what is being moved, how can one know what might be changed?" he says.

Keep regular interval images and snapshots of everything, and be prepared to obliterate anything that is acting abnormally. "One bad apple can spoil the bucket with SDN," Cunningham says. "Make sure that even seemingly benign items, such as virtual routers and databases, are only talking to what they need to talk to for operations. There should be no holes or open ports that aren't needed."

### **Take advantage of threat intelligence**

Security threat intelligence can help alert IT managers about new threats to SDN environments. This type of information is available through a large and growing number of sources that are either included with security tools or are available through stand-alone services.

These resources can help you proactively keep up on the latest threats, particularly those most likely to hit your company or industry.

"We use our expansive view of the threat landscape to set a baseline for normal traffic," Richter says. "The nascent but quickly developing area of threat intelligence is key to navigating the escalating cyber landscape we face."

Keep your network security programme up to date. Security is not static, and with SDN there will be ongoing changes in threats and vulnerabilities, and in the tools used to keep systems secure.

You should upgrade your defenses as new products become available, and update your policies to reflect new realities.

"Security is an ongoing business; do not set it and forget it," Mesceda says. Unfortunately, not everyone heeds that advice. "Often, critical patches are not deployed, systems are not re-evaluated often enough. And the architecture can quickly become vulnerable without a dedicated approach to security," he says. "Many companies use a phased rollout approach, but they fail to revisit earlier rollouts to ensure the system still adheres to security best practices." ■



# HOW TO BUILD PHYSICAL SECURITY INTO A DATA CENTRE

Mantraps, access control systems, bollards and surveillance. Your guide to securing the data centre against physical threats and intrusions.

**T**here are plenty of complicated documents that can guide companies

through the process of designing a secure data centre—from the gold-standard specs used by the federal government to build sensitive facilities like embassies, to infrastructure standards published by industry groups like the Telecommunications Industry Association, to safety requirements from the likes of the National Fire Protection Association. But what should be the CSO's high-level goals for making sure that security for the new data centre is built into the designs, instead of being an expensive or ineffectual afterthought?

Read below to find out how a fictional data centre is designed to withstand everything from corporate espionage artists to terrorists to natural disasters. Sure, the extra precautions can be expensive. But they're simply part of the cost of building a secure facility that also can keep humming through disasters.

**1. Build on the right spot.** Be sure the building is some distance from headquarters (20 miles is typical) and at least 100 feet from the main road. Bad neighbours: airports, chemical facilities, power plants. Bad news: earthquake fault lines and (as we've seen all too clearly this year) areas prone to hurricanes and floods. And scrap the "data centre" sign.

**2. Have redundant utilities.** Data centres need two sources for utilities, such as electricity, water, voice and data. Trace electricity sources back to two separate substations and water back to two different main lines. Lines should be underground and should come into different areas of the building, with water separate from other utilities. Use the data centre's anticipated power usage as leverage for getting the electric company to accommodate the building's special needs.

**3. Pay attention to walls.** Foot-thick concrete is a cheap and effective barrier against the elements and explosive devices. For extra security, use walls lined with Kevlar.



**4. Avoid windows.** Think warehouse, not office building. If you must have windows, limit them to the break room or administrative area, and use bomb-resistant laminated glass.

**5. Use landscaping for protection.** Trees, boulders and gulleys can hide the building from passing cars, obscure security devices (like fences), and also help keep vehicles from getting too close. Oh, and they look nice too.

**6. Keep a 100-foot buffer zone around the site.** Where landscaping does not protect the building from vehicles, use crash-proof barriers instead. Bollard planters are less conspicuous and more attractive than other devices. Or you could do as Apple and Google have done in hiring security guards.

**7. Use retractable crash barriers at vehicle entry points.** Control access to the parking lot and loading dock with a staffed guard station that operates the retractable bollards. Use a raised gate and a green light as visual cues that the bollards are down and the driver can go forward. In situations when extra security is needed, have the barriers left up by default, and lowered only when someone has permission to pass through.

**8. Plan for bomb detection.** For data centres that are especially sensitive or likely targets, have guards use mirrors to check underneath vehicles for explosives, or provide portable bomb-sniffing devices. You can respond to a raised threat by increasing the number of vehicles you check perhaps by checking employee vehicles as well as visitors and delivery trucks.

**9. Limit entry points.** Control access to the building by establishing one main entrance, plus a back one for the loading dock. This keeps costs down too.

**10. Make fire doors exit only.** For exits required by fire codes, install doors that don't have handles on the outside. When any of these doors is opened, a loud alarm should sound and trigger a response from the security command centre.

**11. Use plenty of cameras.** Surveillance cameras should be installed around the perimeter of the building, at all entrances and exits, and at every access point throughout the building. A combination of motion-detection devices, low-light cameras, pan-tilt-zoom cameras and standard fixed cameras is ideal. Footage should be digitally recorded and stored offsite.

**12. Protect the building's machinery.** Keep the mechanical area of the building, which houses environmental systems and uninterruptible power supplies, strictly off limits. If generators are outside, use concrete walls to secure the area. For both areas, make sure all contractors and repair crews are accompanied by an employee at all times.

**13. Plan for secure air handling.** Make sure the heating, ventilating and

air-conditioning systems can be set to recirculate air rather than drawing in air from the outside. This could help protect people and equipment if there were some kind of biological or chemical attack or heavy smoke spreading from a nearby fire. For added security, put devices in place to monitor the air for chemical, biological or radiological contaminant.

**14. Ensure nothing can hide in the walls and ceilings.** In secure areas of the data centre, make sure internal walls run from the slab ceiling all the way to subflooring where wiring is typically housed. Also make sure drop-down ceilings don't provide hidden access points.

**15. Use two-factor authentication.** Biometric identification is becoming standard for access to sensitive areas of data centres, with hand geometry or fingerprint scanners usually considered less invasive than retinal scanning. In other areas, you may be able to get away with less-expensive access cards.

**16. Harden the core with security layers.** Anyone entering the most secure part of the data centre will have been authenticated at least three times, including:

- a.** At the outer door. Don't forget you'll need a way for visitors to buzz the front desk.

- b.** At the inner door. Separates visitor area from general employee area.

- c.** At the entrance to the "data" part of the data centre.

**17. Watch the exits too.** Monitor entrance and exit—not only for the main facility but for more sensitive areas of the facility as well. It'll help you keep track of who was where when. It also helps with building evacuation if there's a fire.

**18. Prohibit food in the computer rooms.** Provide a common area where people can eat without getting food on computer equipment.

**19. Install visitor rest rooms.** Make sure to include bathrooms for use by visitors and delivery people who don't have access to the secure parts of the building. ■



# HOW TO ASSESS THE SECURITY OF SAAS APPLICATIONS

The seven goals a SaaS security review should address  
by Ken Asher, Sales Engineer, Security, Smartsheet



E

nterprises have made many attempts to standardise the

security evaluation of SaaS applications, including establishing certifications to improve clarity and normalise risk, purchasing compliance suites, and building frameworks to keep all of the information aligned, but none of these attempts have succeeded in establishing consistency. Organisations need a model that will effectively assess every type of SaaS application so comparisons can be made across the board.

In order to develop a comprehensive understanding of risk, there are a few key elements that must be fulfilled. Without these elements, it will be much more challenging for to develop a thorough understanding of risk. Unfortunately, these elements are often the most difficult to fulfill.

The first is corroborating data. Most IT departments conduct vendor security assessment in a vacuum without adequate information. Each auditor may have a piece of the overall puzzle, but none actually see the bigger picture because they rarely collaborate and typically only assess vendor security once before purchasing a solution, meaning that they make risk conclusions with what amounts to single data points on vendor controls.

The second element is a comprehensive view of the SaaS vendor's security practices. Some SaaS vendors are reluctant to provide auditors the full details of their security practice for fear it may lead to reduced efficacy of their security controls. For example, exposing the details about an encryption implementation might allow attackers to devise a plan to break the encryption, so vendors are often hesitant to reveal this information. As a result, IT departments don't have a complete understanding of the security controls the vendor has in place.

The final element that is often

missing is the means to measure the effectiveness of audit control questions, assessment frameworks, and the auditors themselves. Currently, the only surefire feedback assessors receive is a vendor data breach.

### **SaaS vendors' perspective on security assessment**

SaaS vendors' business often hinges on a successful security assessment outcome so it's in their best interest that their prospects have available an effective evaluation process for security practices. Such a process is likely to lead to appropriate, well-informed risk decisions by buyers. Conversely, inconsistent assessment questions, auditor inefficacy, and inaccurate risk conclusions will be detrimental to widespread SaaS adoption.

In addition, many SaaS vendors are impacted by a lack of a standard method for assessing vendor security, meaning that every assessment has unique questions that must be carefully reviewed and answers must be crafted and considered. This makes the process much more tedious and labor intensive.

Clearly, it is in the best interest of both SaaS vendors and organisations' IT departments to establish a consistent risk-evaluation process. So how can this be accomplished? First, let's consider the key goals:

1. Relieve some of the vendors' labor burden to complete security assessments
2. Make more data available to the assessors
3. Standardise and improve the quality of audit questions
4. Measure and improve assessor capabilities
5. Transform stand-alone audit into consensus audit
6. Reduce the cost of a high-quality audit
7. Improve the ability of small businesses to make informed risk decisions

The most effective solution would be one that accomplishes all seven goals. The solution could be developed in a variety of different environments, say within an existing GRC (governance, risk management, and compliance) tool, or in an Excel document, a Smartsheet, or even simply as a security audit list in Microsoft Word.

It can be accomplished by using a method that would enable IT departments to collaborate on their assessment of vendors with their peers. The solution should include assessment and assessor peer review, assessment question categorisation and rate-and-comment capabilities, and a means to protect vendor security practice while making collaborative assessment information available to the public. This information would give auditors much-needed corroborating evidence to help them understand the risk for each functional control area.

This approach (simplified here for brevity) would also give customers the ability to compare their own results against the established community baseline for each functional control area. That would allow them to draw conclusions related to the efficacy of their own auditors and the relative strength of their assessment process. Additionally, making collaborative assessment information public allows small businesses that don't have sophisticated information security departments to make informed risk decisions when purchasing software.

Everyone from SaaS vendors to potential buyers of every stripe can benefit from increased collaboration and vendor transparency. Implementing a collaborative solution would significantly improve the security assessment process and provide benefits for enterprises, small businesses, and SaaS vendors by allowing IT departments to enable their line-of-business leaders to find and purchase business enablement solutions with confidence knowing that their data is protected. ■



*Cricket Liu, Chief DNS  
Architect, Infoblox*

# FIGHTING CYBERWARFARE

[ by Kasey Cross, Sr. Product Marketing Manager at A10 Networks ]

# S

tate-sponsored cyber-attacks strike with shocking frequency. The motives, methods

and results of these state-sponsored attacks vary, but the implications are clear: Every organisation that stores sensitive information has a proverbial bullseye on its back. Well-funded and extremely efficient, with seemingly unlimited resources and talent at their disposal, state-sponsored cyber criminals would appear to be an unbeatable foe.

Well, there are various ways government enterprises in the Middle East can protect themselves. Here is a more detailed look at what government agencies should do to keep nation-state attackers at bay.

## Decrypt and inspect SSL traffic

State-sponsored hackers can hide attacks in encrypted SSL traffic to evade detection. As a result, network security solutions, such as next-gen firewalls and intrusion prevention systems, need to be able to inspect all incoming and outgoing traffic for threats, not just the data that is sent in plain text. What you can't see can hurt you. To ensure state-sponsored hackers do not bypass your security controls, decrypt and examine all traffic.

Below are five features for IT teams to consider when selecting an SSL inspection platform:

**SSL performance:** In addition to assessing current Internet bandwidth requirements, IT also must factor in SSL traffic growth and ensure the inspection platform can handle future SSL throughput requirements.

**Compliance:** To address regulatory requirements like HIPAA, Federal Information Security Management Act (FISMA) and Sarbanes-Oxley (SOX), an SSL inspection platform should be able to bypass sensitive traffic, like traffic to banking and healthcare sites.

**Heterogenous networks:** IT should look for SSL inspection platforms that can decrypt outbound traffic to the Internet and inbound traffic to corporate servers with multiple, flexible deployment options. Additionally, the platforms should intelligently route traffic

with traffic steering, granularly parse and control traffic-based on custom-defined policies and integrate with a variety of security solutions from leading vendors.

**Security infrastructure:** SSL inspection platforms should not just offload SSL processing from security devices but also maximise the uptime and performance of those devices. It's important the platforms can scale security deployments with load balancing, avoid network downtime by detecting and routing around failed security devices and support advanced health monitoring to rapidly identify network or application errors.

**SSL certificates and keys:** To ensure certificates are stored and administered securely, IT should look for SSL inspection platforms that provide device-level controls to protect SSL keys and certificates, integrate with third-party SSL certificate management solutions and support FIPS 140-2 Level 2 and Level 3 certified equipment and Hardware Security Modules (HSMs).

## Fortify Web applications against attacks

Web application data is an attractive target for state-sponsored hackers. Attackers have been known to exploit application vulnerabilities to gain access to Web servers or steal records from databases. One way agencies can protect against this is with a certified Web application firewall (WAF), which filters all application access by inspecting both the traffic toward the application and the response traffic from the application.

A WAF offers granular control of the application's data flow and is capable of protecting against various attacks including SQL injection, cross-site scripting (XSS) and cross-site request forgery (CSRF) attacks, among others. For instance, a WAF can prevent buffer overflow attacks by setting accepted maximum thresholds for aspects of HTTP requests and blocking requests that exceed the configured limits.

## Use Virtual Private Networks (VPNs) to secure data

You should assume that any communications over public networks can and will be intercepted. Therefore, agencies of all sizes should implement

IPsec VPNs to prevent snooping and data theft, as well as to address compliance. Though it's no guarantee your data will be protected, you should still encrypt sensitive data sent over the Internet using IPsec encryption.

While IPsec is a mature and well understood technology, new networking paradigms like cloud computing, as well as escalating bandwidth requirements, are compelling large enterprises and service providers to rethink their VPN strategies. As a result, agencies need to develop VPN architectures that can:

- Support unprecedented IPsec throughput levels
- Leverage BGP routing for high availability and rapid scaling
- Spin up new IPsec tunnels and gateways on-demand in cloud environments
- Minimise power consumption and rack space requirements for data center efficiency

## Monitor and audit access to sensitive data

If you store sensitive data in databases or files, be sure to track all activity including access and changes. This will help detect anomalous activity, prevent illicit access and measure the impact of an intrusion if an incident does occur. Monitoring and auditing user access to sensitive data ensures there is a trail to link security violations to specific user names.

## Train employees on security best practices

Your own employees will often be your weakest security links. Therefore, it's important for organisations to educate their teams and enforce best practices, such as choosing a strong password, to prevent advanced cyber attacks. Users should also be instructed to identify social engineering attacks, phishing threats and other malicious activity. Otherwise, they'll likely become a victim.

The world has changed. The lone hacker is no longer the face of cybercrime. That bad actor has been replaced by entire nation states with dedicated professional teams of infiltrators. They are formidable. They are relentless. They are coming for your data.

Protect it. ■





Zulfikar Ramzan, CTO  
of RSA Security

# MODERN DEFENCE

Zulfikar Ramzan, CTO, RSA Security, discusses how organisations should change their mind-sets to adapt to the evolving threat landscape and the value add security can bring to businesses.

**T**

**his is the first time that the RSA Conference is being held in this part of**

**the world. What prompted you to hold the event here?**

We are always looking at how we can inculcate the worldwide community of security professionals and vendors, and get them to come to one place. While it will be very easy for the Conference to be held in just one location every year, we felt that that would limit our opportunity to create that community. I believe that cybersecurity is not an issue that affects only one individual, this is a subject that can impact anybody in different ways.

I am particularly excited to have come to this part of the world because

economies in this region are heading towards rapid growth. There has been a tremendous change in this region during the last 10 to 15 years and almost everything has transformed. I think that is a sign of the progressively changing times.

When I look at burgeoning economies, wherever part of the world that may be, they all have one thing in common – they are all encumbered by legacy issues. Nevertheless, they are forward thinking when it comes to improving the IT landscape and that excites me as a technologist. We are seeing that a lot of our customers here are starting to really understand and accept the way the threat landscape is shifting.

**Last year at the RSA Conference your president Amit Yoran mentioned that security is still stuck in the Dark Ages. What do you think he meant by that?**

I think that's because of incumbency issues. A lot of companies are still encumbered by traditional security systems. If you look at security 20 years ago, security mainly focuses on two elements – firewall and antivirus.

For the longest time that has been sufficient, there were not that many threats then and they pretty easy to deal with. Overtime, security evolved with elements such as IPS, IIDS and so on. But ultimately, the goal of every organisation is to know how they can prevent attacks from happening and how they can protect everything that is within the walls of their

perimeter. However, the threat landscape has radically transformed since then and cybercriminals have also changed. As a result, the same technologies that they have relied on for so many years started failing them in unprecedented ways, and yet a lot of these organisations remain reluctant to changing their mind-set.

There was a recent study by Forrester which identified that when most IT leaders budget their spending they focus more on prevention technologies. This should not be the case because they are merely putting more effort on building taller walls and digging deeper moats which will not solve the problem entirely. That is the message that we are trying to get across, organisations should move beyond these traditional mechanisms and embrace the way the landscape has evolved.

I'm not saying that they shouldn't have an antivirus or a firewall, but they must not mistake these technologies as proper strategies for dealing with advance threats. The most aggressive and impactful threats can only be addressed by a comprehensive strategy, which involves analytics as this can will help organisations gain insights on their visibility. This should then lead to a comprehensive governance programme, so that they can take the low-level technical issues and translate them up to high-level business risks. Because the one thing that we are seeing nowadays is that cybersecurity is no longer dedicated to just the realm of the highly technical specialist, it has now become a crucial element to every member of the C-suite and management teams.

The CEOs and CFOs may not care about the technical implications of a malware but they do care about how it will translate to business operations, what risks it will bring and how they can compensate for it. We have to take the language of IT security professionals and translate that the language that C-level members understand. Enterprise leaders are now recognising security as a critical business issue. At the same time, CIOs and CISOs are increasingly being asked to use security in bringing more value to the business.

**One of the problems of security today is the increasing number of alerts and false positives. People cannot identify which specific alerts they should pay attention to. Is this where security analytics come to the picture?**

Absolutely. If you look at some of the major breaches during the last 18 months, every one of them had the technology that you would expect when it comes to security. They had SIEM, next-gen firewalls, Sandbox and so on. Those technologies failed them when the breaches happened.

Now, part of why they failed is because they had numerous of alerts. They might have pinpointed some critical issues but they also found 5000 other things that were not entirely relevant. So, when you see 5000 alerts what do you do?

The way I see it is like this, if you have an alert that has no context that alert is useless. You need to have some context around that alert. If you have the extra visibility you can triage these alerts and find out which ones actually matter.

So, having a deep and pervasive visibility helps you eliminate irrelevant alerts.

You can still further simplify this. Organisations can juxtapose these alerts with business context and through this process they can find out which ones are impacting their most critical data. Upon doing so, they can have their IT security teams assess and address these alerts.

With the right combination of security analytics, pervasive visibility and having the business context organisations can eliminate irrelevant threat elements and focus on the most critical issue. In doing so, they'll be able to concentrate on how they can address these critical problems and improve their risk posture.

**What can you say is the ideal security posture?**

I think there should be an equitable split on investment between prevention, detection and response technologies.

Make sure you also have a good identity access management. Identity is the first key pillar to having a good security posture. As we move into a world where the perimeter becomes less and less relevant, identity is one of the last tangible things you can hang onto from the security perspective. If you look at it closely, identity is a cornerstone of security. Because security has always been about the assertion of ensuring that only the right people can access the right resources at the right time.

The second key pillar is visibility. Understand where the attackers are trying to get into and identify it earlier in the kill chain. Know that intrusion is very much different from a breach. While you cannot stop all incidents of intrusion, you can always find a way to stop cases of breaches. That should be the goal of every organisations from the security standpoint. You have to figure out how to minimise the impact of an intrusion and reduce the risks of attackers taking your most critical assets.

The final component is making sure you can translate this to business risk. Because ultimately, security is part of a pervasive culture in an organisation and an integral business critical aspect of a company. 📌

**“With the right combination of security analytics, pervasive visibility and having the business context you can eliminate irrelevant threat elements and focus on the most critical issue.”**



*Cricket Liu, Chief DNS Architect, Infoblox*

# SECURING THE NETWORK

Cricket Liu, Chief DNS Architect, Infoblox, discusses the potential of passive DNS in protecting network infrastructure.



**T**

he number of attacks against Domain Name

System (DNS) infrastructure has grown exponentially in recent years, having increased by 200 percent since 2012. Exploiting this vulnerable infrastructure is a popular, and often very successful, tactic for causing disruption to organisations.

The popularity of DNS as a target is unsurprising considering its high value to business operations: companies are unable to conduct business online without DNS functioning properly. And with traditional protection, like firewalls, leaving port 53 open, networks are constantly being exploited via DNS for a variety of criminal purposes.

Examples of attacks include DDoS (distributed denial of service) attacks against authoritative name servers, the use of name servers as amplifiers in DDoS attacks, cache poisoning attacks, the use of compromised registrar accounts to modify delegation information, and abuse of name servers by malware.

Fortunately, given the plethora of potential attack vectors, new and powerful mechanisms are being developed to help organisations combat these threats. These include the DNS Security Extensions, Response Rate Limiting and Response Policy Zones.

But what looks to be one of the most promising methods for enhancing DNS security – and, as a result, the security of the Internet more generally – remains to be fully exploited. This is Passive DNS data.

### **Appropriating Passive DNS data**

Invented in 2004 by security researcher Florian Weimer, Passive DNS was developed as a method for combatting malware. Logging the

responses received from other name servers, the recursive name servers then would replicate said logged data to a central database.

To get an idea of what this logged data would look like, recall how recursive name servers work. When queried, these servers examine both their authoritative data and cache for an answer. If this information is not present, the servers by default will begin by querying one of the root name servers, continuously following referrals until they are able to identify those authoritative name servers that know the answer and then retrieve it from one of these servers.

Passive DNS data consists of all the information collected throughout this process. This largely consists of the referrals and answers from the contacted authoritative name servers on the Internet, and of course any errors. All this data is time stamped, deduped, compressed, and replicated to a central database where it is archived and analysed.

It is worth specifying at this point that the captured data is server-to-server communication and not queries from stub resolvers to the recursive name server. This is an important aspect of Passive DNS, as it means that there is significantly less server-to-server talk than there is between a stub resolver and a recursive name server. It also represents less of a privacy concern, as the server-to-server communication cannot easily be associated with a specific stub resolver.

The Passive DNS data can be collected in various ways. Some recursive servers, such as Knot and Unbound, actually have software hooks that make Passive DNS data capture especially easy. Using a free programme called dnstap ([http://](http://dnstap.info/)

[dnstap.info/](http://dnstap.info/)), administrators are able to read the Passive DNS data from the name server.

For those running other name servers, there are different tools they can use on the host running the recursive name server to monitor traffic to that name server, or to mirror the port of the name server to another host which in turn records the data.

### **Uploading the data**

There are a number of organisations that run the databases which Passive DNS data “sensors” can upload data to. One of the most well known and popular of these is Farsight Security’s Passive DNS database, otherwise known as DNSDB. This database contains the data collected from sensors all over the world for more than several years. Passive DNS databases are also run by organisations including VirusTotal, which is now owned by Google; BFK, the German consultancy firm; RiskIQ’s PassiveTotal; Estonia’s Computer Emergency Response Team, CERT-EE; and the Computer Incident Response Center Luxembourg (CIRCL).

Querying these Passive DNS databases allows network administrators to determine which queries returned a specific IP address in any given month, discover which name servers a particular zone used at some point in the past, and even what other zones use that same set of name servers.

Perhaps more significantly, however, is the ability to take an IP address that you know to be malicious and identify all the other domain names that the Passive DNS sensors map to that specific IP address.

### **Putting the data to use**

While this information has numerous

benefits for network administrators in gaining a greater understanding of an organisation's DNS and drilling down into the background of specific IP addresses, Passive DNS data can also be exploited to protect against data exfiltration and compromise by malicious domains.

One example is enabling an organisation to detect cache poisoning and fraudulent changes to delegation in near real time. By periodically querying a Passive DNS database, an organisation would use information garnered by Passive DNS sensors to find what addresses its critical domain names currently map to. An organisation would then be able to distinguish any variation from the mappings in authoritative zone data, which is a common indication of compromise.

Another means by which Passive DNS databases can help prevent malicious domains infiltrating an organisation's network through DNS queries is by blocking new domain names. A high correlation has been identified between brand new domain names and malicious activity. This is because these domains are frequently used only briefly in phishing campaigns or other similar attacks, before being discarded. As such, Farsight Security periodically scrapes the newest domain names from DNSDB, for instance those which were first identified by DNS sensors in the preceding 15 minutes, hour, or other interval. This can provide organisations with a feed of these new, potentially malicious domain names, enabling network administrators to block their resolution. The cost of temporarily blocking the few newly-created legitimate domain names that happen to have appeared in the last 15 minutes is a small price to pay for safer networks.

Monitoring domain names which change their addresses is another technique which helps detect malware

**“The Passive DNS data can be collected in various ways. Some recursive servers, such as Knot and Unbound, actually have software hooks that make Passive DNS data capture especially easy.”**

and phishing sites. Legitimate domain names change their address very infrequently, aside from those used for load balancing and distribution. By keeping track of any changes to address (A and AAAA) records and name server (NS) records, it is possible to identify which domains are using techniques like fast flux to help malicious servers evade detection.

And once a name server or IP address is marked as malicious, it is very simple for a Passive DNS database to identify other potentially malicious domain names that have mapped to that IP address.

Finally, if an organisation deploys a

Passive DNS database which supports Soundex or fuzzy matching, it would be able to query that database periodically for domain names that use or sound like its trade names. This will help them identify potential infringement.

### **Using Response Policy Zones to close the loop**

Response Policy Zones, or RPZs, are DNS zones whose contents are interpreted as policy rules. These rules typically say things along the lines of “For anyone trying to look up A records for this domain name, return an error saying that this domain name doesn't exist.” RPZs are an invaluable mechanism in closing the loop when malicious domain names are identified in Passive DNS data.

As RPZs are just zones, they can be quickly and efficiently transferred around the Internet, and the policies that they contain can be rapidly enforced. Organisations can analyse Passive DNS data to identify malicious domain names, and then construct rules blocking the resolution of these names and distribute those rules to subscribers around the Internet.

### **First steps**

If you are interested in contributing Passive DNS data from your recursive name servers, Farsight provides information on how to participate and includes a step-by-step guide for setting up a Passive DNS sensor. It is also possible to add RPZ feeds - based on the analysis of Passive DNS data - to aid in blocking the resolution of malicious domain names in your organisation.

We're still working to understand the full potential of Passive DNS data, but the insight that it provides and the value that this intelligence offers to network administrators demonstrates that it will play a key role in securing this important, yet vulnerable, part of network infrastructure in years to come. **■**

future  
technology  
week

THE **Big**  
DATA SHOW

IoT*x*

Four live shows:



**GISEC**  
GULF INFORMATION SECURITY EXPO & CONFERENCE  
معرض ومؤتمر الأمن المعلوماتي الخليجي

**GEMEC**  
معرض ومؤتمر الموبايل الخليجي للخدمات  
GULF ENTERPRISE MOBILITY EXHIBITION & CONFERENCE

future  
technology  
week.

29-31  
march 2016

4 live events showcasing the  
technology innovations that  
are reshaping our world.

Free to attend:

**Hackathon | Market Labs  
Capture the Flag | The Hive  
Interactive Arena**

ORGANISED BY



**GET YOUR FREE  
VISITOR PASS  
TODAY.**

[www.futuretechweek.com/visit](http://www.futuretechweek.com/visit)





Ahmed Qurram Baig,  
Founder, CISO Council

# NEXT-GEN CYBERSECURITY LEADERS

**T**he digital transformation of businesses globally, with emergence of Smart Cities is changing the very definition of security role, from being a technology centric to more of a business-centric executive role, forcing the security leaders to get more involved and be responsible for securing business processes and operational technologies that control Smart Cities and critical infrastructure of a nation.

The seriousness of any business with regard to security starts with commitment to invest in a CISO or security executive, even though in some cases existing employees without appropriate knowledge or experience are simply re-casted in this new role. This is usually done for compliance or as response to audit findings or recommendations.

The challenges and interaction of CISOs get much wider and risks emerge from across different business domains. The security threats today are from more organised crime industry and nation-state actors which demands CISO to understand and manage digital technology adoption and transformation with business objectives, legal and regulatory landscape in mind.

The modern enterprise demands ubiquitous connectivity and freedom to work from anywhere, anytime on any device, making it a virtually perimeter less organisation with humans acting as perimeter and first line of defense.

CISOs today are becoming part of the deadliest catch category (most

dangerous / riskiest jobs), fighting against a lot of unknown and unexpected threats, only way to succeed here against all the threats is to act as a group or a community, by supporting and sharing knowledge and intelligence. While, the CISO requires to build trust with executive management through thought leadership, understanding of business issues and translating the technology risks into business language, it needs to be supported with necessary information / reports and actionable intelligence to gain attention from the management.

The new generation of CISOs as executives are required to be more social and business friendly with excellent communication and presentation skills especially as they are now part of boardroom discussion and decisions. CISO's are not expected to be a geek working behind a closed door, trying to secure and protect the business and CISO's who tend to use fear, uncertainty or doubt without interacting with business executives and other teams can be ostracised and might fail eventually.

Here are a few recommendations for our CISO Council members and Security Executives Community to enhance their role.

**Connect:** Connecting with industry players and peers with similar interest and business risks will allow you to discuss and learn from their success or failures. Also, connecting with cross-industry and cross-continental security leaders will open up new ideas of protection strategies and allow you to

be innovative in your security strategies.

**Collaborate:** CISO networking platforms and security events are good source to learn about new technologies and most importantly meet other security leaders in person. Peer interactions and deliberation are helpful to gain different perspectives to addressing security risks, it would also allow you better manage your security initiatives by learning different ways of doing same things from different organisations.

**Contribute / Share:** The power of sharing information is invaluable, the only way, you can beat the adversary is by learning his techniques and actions. This can be more effective as a community that shares information with each other and partnerships from industry service providers. CISO roundtables and other closed-door sessions have also proven to be very effective.

**Learn:** Learning and professional development should be integral part of individual growth and way to get familiar with advances in technology and other business practices. The vast experience and knowledge gained by global industry leaders, that is available through books, courses, conferences and articles will prove to be very helpful against all odds to overcome challenges.

The current demand for security executives and lack of availability will force organisations to invest more in external support and train internal leaders. The future CISOs or next-generation security executives would emerge from various disciplines and experiences. 📌

# Lead with Arrow!

The Premier Storage & Security Distributor in the Middle East.



More than 10 years'  
experience in the Middle East



100+ employees  
in the region

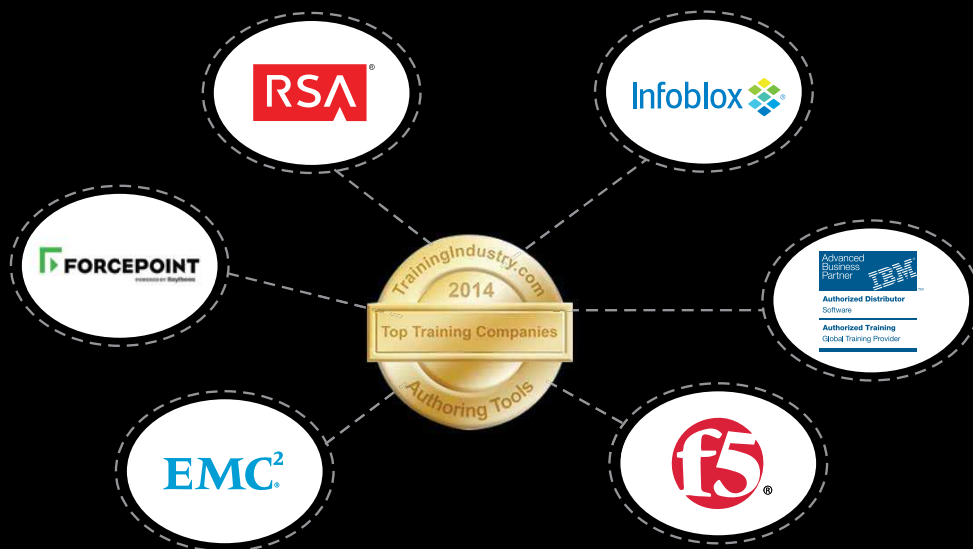


Dedicated teams in KSA-Gulf-  
Pakistan- Levant and North Africa



400 + resellers

Arrow ECS Authorized Training Center for the following products



- Fully equipped Demo center in Arrow ECS office in Dubai.
- Advanced technical capabilities for pre-sales proof of concept installation support

EMC<sup>2</sup>

RSA

VCE

IBM

Infoblox

Arrow

TREND  
MICRO

intel Security

f5

FORCEPOINT  
powered by Raytheon

Five Years Out

For any inquiry or more information, please contact us on

marketing-ae@arrowecs.ae

P: +971 4 5015814 F: +971 4 501 5837

<http://www.arrowecs.ae>

# Secure Your Network with Fortinet

Protecting today's enterprise takes more than just implementing best of breed technologies in the network. Changes in the corporate IT environment can open up new security holes. And more complex Internet threats increasingly bypass the first line of defense.

This evolution calls for a new approach to network security. A holistic, end-to-end solution is crucial to ensure the protection of the total IT infrastructure – from the desktop to the datacenter and from the campus to the branch office – with all elements of the solution working collaboratively.

Built for security and performance, only Fortinet can secure the entire network, ensuring the safety and integrity of the corporate data.

**Join the more than 225,000 organizations worldwide that have already chosen Fortinet to secure their most critical business assets.**



SECURED BY  
**FORTIGUARD®**

## **Fortinet Solutions include:**

- A comprehensive range of high performance firewalls to meet all network requirements
- Advanced Threat Protection
- Web Application Firewall
- Secure Wireless Networking
- Email Security
- DDoS Protection

[www.fortinet.com](http://www.fortinet.com)